UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,368	01/09/2004	Richard A. A. Heylen	224.	7594

31665 7590 06/14/2007

PATENT DEPARTMENT
MACROVISION CORPORATION
2830 DE LA CRUZ BLVD.
SANTA CLARA, CA 95050

EXAMINER	
SHAIFER HARRIMAN, DANT B	
ART UNIT	**PAPER NUMBER**
2109	
MAIL DATE	**DELIVERY MODE**
06/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/754,368	HEYLEN, RICHARD A. A.	
	Examiner	Art Unit	
	Dant B. Shaifer - Harriman	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/09/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :07/05/2005, 06/27/2005,08/27/2005.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: on page 12, line 14 of the specification the word "organisations," should be spelled "organizations." .

Appropriate correction is required.

Claim Objections

2. Claim(s) 11 is objected to because of the following informalities: the phrase altered codeword" doesn't necessarily mean "altered values." Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claim(s) 15 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The examiner points out that a data file contains only static data not active data (i.e. word documents, excel spread sheets etc.) The examiner notes that it is awkward for a data file to contain a command library, command shell interpreter. For examining purposes, the examiner will treat the executable as a file that contains data.

Claim(s) 1- 27 are rejected as failing to define the invention in the manner required by 35 U.S.C. 112, second paragraph.

The claim(s) are narrative in form and replete with indefinite and functional or operational language. The structure, which goes to make up the device, must be clearly and

positively specified. The structure must be organized and correlated in such a manner as to present a complete operative device. The claim(s) must be in one sentence form only. Note the format of the claims in the patent(s) cited. Furthermore, function that is currently cited in the instant claims of the applicant are of the form the leads them to be executed in the past and not in the present, upon the claims being corrected, the applicant must write the claims in the present. An example would be, claim 16, page 24 of the disclosure, which states "A medium on which copy protected encoded digital data has been stored," it should read "A medium on which copy protected encoded digital data is stored." Furthermore the applicant must with regards the method claims, start with an action verb. For example, an action verb is comprises or consists of. Finally, the applicant must with reference to apparatus and device claims should list out the components of the applicants claimed invention. For example, a watch has band, band fastener, hour hand, minute hand etc.

Claim(s) 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Furthermore, the examiner for examining purposes is treating "large magnitude" as the upper nibble of a data byte.

Claim(s) 1-27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Furthermore with regard to the independent claims, as well as each dependent claim, which depends on the independent claim in question, "altering values of bytes of a codeword,"

the word codeword could be a algorithm, text, numbers. Specifically, a byte can be a text or a number, applicant must be more specific to what a "altering the values of a codeword," is.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim(s) 14 & 15 are rejected under 35 U.S.C. 101 because the claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se.*

Claims 16 – 27 are rejected under 35 U.S.C. 101 because the claims merely claiming non-functional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

Claim(s) 16 –27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims(s) 16 -27 are directed to a medium that has stored on it, is a

copy protected encoded digital data that is arranged in codewords, and the data bytes that make up these codewords, are altered in such a manner that when an error correction unit (i.e. usually found in a digital recorder for making illegal copies of digital data) executes to correct that digital data bytes that are corrupted or damage when making the illegal copy of the digital encoded data, the error correction unit will read the altered codeword as uncorrectable, furthermore the altering of the data bytes will prevent the illegal copy from being audible.

This claimed subject matter lacks a practical application of a judicial exception (law of nature, abstract idea, naturally occurring phenomenon) since it fails to produce a useful, concrete and tangible result.

Specifically, the claimed subject matter does not produce a tangible result because the claimed subject matter fails to produce a result that is limited to having real world value rather than a result that may be interpreted to be abstract in nature as, for example, a thought, a computation, or manipulated data. More specifically, the claimed subject matter provides for rendering a codeword uncorrectable through altering the data bytes, by manipulating the higher order and lower order bits of the data byte, altering four or five or more of the data bytes contained in a codeword, Xoring (i.e. exclusive – or) a corrupting vector with a codeword that has all of its data byte values set to zero (indicating that the word has no errors in it), altering the parity bytes of the codeword to achieve an uncorrectable codeword. This produced result remains in the abstract and, thus, fails to achieve the required status of having real world value.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim(s) 1 - 6 & 8 – 10 & 11 & 12 & 14 – 21 & 23 - 26 are rejected under 35 U.S.C. 102(b) as being taught by Sollish et al. (Patent # 6311305 B1).

Sollish teaches:

Claim(s) 1. A method of copy protecting encoded digital data, wherein:

- the encoded digital data has been subjected to error correcting encoding and is arranged in codewords, each codeword containing data bytes and parity values, the method comprising altering the values of the data in a plurality of data bytes in a selected codeword, to form an altered codeword, the nature of the altered values and the number of data bytes altered being chosen to render the altered codeword uncorrectable (Col. 9, lines 15 – 25, the examiner notes that ECC (error correction codeword), meaning that error correction encoding is to take place; to one of ordinary skill in the art, the ECC

contains both symbols (data bytes) and parity bits; how the data bytes are being altered are that at specific CD medium locations, the correctable data bytes are being removed and being replaced with non-correctable data bytes. Thus, when an audio CD is read the error correction unit will mark those "altered" code words as uncorrectable, furthermore bypassing a error correction unit of a CD ROM, can be a means to prevent the unauthorized copying of the CD data.)

Claim(s) 2. A method as claimed in Claim 1, wherein:

- the values of the data in at least four data bytes in the selected codeword are altered(Col. 11, lines 13 –28, the examiner notes that a codeword is altered by replacing correctable data with invalid or uncorrectable data, that would render the codeword uncorrectable to a error correction unit in CD –ROM player, furthermore for effective override of error correction unit that is used in a CD – ROM to read a audio CD, 20 for more correctable bytes must replaced with invalid or uncorrectable data bytes. This implies four or more data bytes are altered with in the codeword.)

The examiner further notes that Claim 17 is rejected under the same logic and reasoning as Claim 2 is rejected under, based on the fact the instructions embedded in the medium of claim 17 is merely the implementation of the method in claim 2.

Claim(s) 3. A method as claimed in Claim 1, wherein:

- the values of the data in at least five data bytes in the selected codeword are altered(Col. 11, lines 13 –28, the examiner notes that a codeword is altered by replacing correctable data with invalid or uncorrectable data, that would render the codeword uncorrectable to a error correction unit in CD –ROM player, furthermore for effective override of error correction unit that is used in a CD – ROM to read a audio CD, 20 for more correctable bytes must replaced with invalid or uncorrectable data bytes. This implies four or more data bytes are altered with in the codeword.)

The examiner further notes that Claim 18 is rejected under the same logic and reasoning as Claim 3 is rejected under, based on the fact the instructions embedded in the medium of claim 18 is merely the implementation of the method in claim 3.

Claim(s) 4. A method of copy protecting encoded digital data, wherein:

- the encoded digital data has been subjected to error correcting encoding and is arranged in codewords, each codeword containing data bytes and parity values, the method comprising altering the values of the data in a plurality of data bytes in a selected codeword, to form an altered codeword, the nature of the altered values and the number of data bytes altered being chosen to render the altered codeword uncorrectable(Col. 9, lines 15 – 25, the examiner notes that ECC (error correction codeword), meaning that error correction encoding is to take place; to one of ordinary skill in the art, the ECC

contains both symbols (data bytes) and parity bits; how the data bytes are being altered are that at specific CD medium locations, the correctable data bytes are being removed and being replaced with non-correctable data bytes. Thus, when an audio CD is read the error correction unit will mark those "altered" code words as uncorrectable, furthermore bypassing a error correction unit of a CD ROM, can be a means to prevent the unauthorized copying of the CD data.), and

wherein:

- one or more higher order bits of each data byte of the plurality of data bytes are altered to be representative of an unusually large magnitude(Col. 9, lines 15 –25, the examiner notes that a symbol is a byte, and a byte is made up of 8 bits, in order to alter or manipulate a byte, the bits or the higher order bits of the byte are manipulated, which is and the only way to alter a data byte into a error symbol, which will then replace a correctable data byte in the codeword according to the present invention, furthermore in plain meaning altering a data byte, also means altering its higher order bits.)

- and the remaining lower order bits of each data byte of the plurality of data bytes are altered such that, on decoding, the altered codeword will generate an uncorrectable error identifying syndrome (Col. 9, lines 15 –25, the examiner notes that a symbol is a byte, and a byte is made up of 8 bits, in order to alter or manipulate a byte, the bits or the lower order bits of the byte are manipulated, which is and the only way to alter a data byte into a error symbol, which will then replace a correctable data byte in the codeword according to the present invention, in plain meaning altering a data byte, also means altering its lower order bits.)

The examiner notes that claim 19 is rejected under the same logic and reasoning that claim 4 is rejected under, furthermore the medium is merely the implementation of the method, which when both the method and the medium is executed the results will be exactly the same.

Claim(s) 5. A method as claimed in Claim 4, wherein:

- the most significant nibble of each data byte of the plurality of data bytes is altered to be representative of an unusually large magnitude(Col. 9, lines 15 –25, the examiner notes that a symbol is a byte, and a byte is made up of 8 bits, the 8 bits when divided by 2 are considered two groups of four, which is called a nibble. A nibble can be either higher or lower order of bits in a byte, in order to alter or manipulate a byte, the nibbles of the byte are manipulated, which is and the only way to alter a data byte into a error symbol, which will then replace a correctable data byte in the codeword, in plain meaning when a data byte is altered to an error or invalid byte, the nibbles of the byte are also being manipulated to achieve these symbols that make a uncorrectable codeword.),

and wherein:

- the least significant nibble of each data byte of the plurality of data bytes is altered to generate the uncorrectable error identifying syndrome on decoding(Col. 9, lines 15 –25, the examiner notes that a symbol is a byte, and a byte is made up of 8 bits, the 8 bits when divided by 2 are considered two groups of four, which is called a nibble. A nibble can be either higher or lower order of bits in a byte, in order to alter or manipulate a byte,

the nibbles of the byte are manipulated, which is and the only way to alter a data byte into a error symbol, which will then replace a correctable data byte in the codeword, in plain meaning when a data byte is altered to an error or invalid byte, the nibbles of the byte are also being manipulated to achieve these symbols that make a uncorrectable codeword.)

The examiner notes that claim 20 is rejected under the same logic and reasoning that claim 5 is rejected under, furthermore the medium is merely the implementation of the method, which when both the method and the medium is executed the results will be exactly the same.

Claim(s) 6. A method of copy protecting encoded digital data, wherein:

- the encoded digital data has been subjected to error correcting encoding and is arranged in codewords, each codeword containing data bytes and parity values, the method comprising altering the values of the data in a plurality of data bytes in a selected codeword, to form an altered codeword, the nature of the altered values and the number of data bytes altered being chosen to render the altered codeword uncorrectable(Col. 9, lines 15 – 25, the examiner notes that ECC (error correction codeword), meaning that error correction encoding is to take place; to one of ordinary skill in the art, the ECC contains both symbols (data bytes) and parity bits; how the data bytes are being altered are that at specific CD medium locations, the correctable data bytes are being removed and being replaced with non-correctable data bytes. Thus, when an audio CD is read the error correction unit will mark those "altered" code words as uncorrectable, furthermore

bypassing a error correction unit of a CD ROM, can be a means to prevent the unauthorized copying of the CD data.),

and wherein:

- the nature of the altered values and the number of data bytes altered are chosen such that, on decoding, the altered codeword will generate an uncorrectable error identifying syndrome(Col. 9, lines 15 – 25, the examiner notes that as the error correction decoder scans the data sectors of the CD or medium, any and all (syndrome) non-correctable error pattern will be identified as uncorrectable and will remain unaltered, furthermore for examination purposes the examiner will is construing the word "syndrome" as, merely a reoccurring event (i.e. every time with a uncorrectable codeword is detected by the CD – ROM error correction detector unit, it will regard the codeword as uncorrectable and the erroneous codeword will remain unaltered.)

The examiner notes that claim 21 is rejected under the same logic and reasoning that claim 6 is rejected under, furthermore the medium is merely the implementation of the method, which when both the method and the medium is executed the results will be exactly the same.

Claim(s) 9. A method of copy protecting encoded digital data, wherein:

- the encoded digital data has been subjected to error correcting encoding and is arranged in codewords, each codeword containing data bytes and parity values(Col. 9, lines 15 – 25, the examiner notes that ECC (error correction codeword), meaning that error

correction encoding is to take place; to one of ordinary skill in the art, the ECC contains both symbols (data bytes) and parity bits; how the data bytes are being altered are that at specific CD medium locations, the correctable data bytes are being removed and being replaced with non-correctable data bytes. Thus, when an audio CD is read the error correction unit will mark those "altered" code words as uncorrectable, furthermore bypassing a error correction unit of a CD ROM, can be a means to prevent the unauthorized copying of the CD data.),

the method comprising:

- altering the values of the data in a plurality of data bytes in a selected codeword, to form an altered codeword, the nature of the altered values and the number of data bytes altered being chosen to render the altered codeword uncorrectable(Col. 9, lines 15 – 25, the examiner notes that ECC (error correction codeword), meaning that error correction encoding is to take place; to one of ordinary skill in the art, the ECC contains both symbols (data bytes) and parity bits; how the data bytes are being altered are that at specific CD medium locations, the correctable data bytes are being removed and being replaced with non-correctable data bytes. Thus, when an audio CD is read the error correction unit will mark those "altered" code words as uncorrectable, furthermore bypassing a error correction unit of a CD ROM, can be a means to prevent the unauthorized copying of the CD data.),

and wherein:

- one or more higher order bits of each data byte of the plurality of data bytes are altered to be representative of an unusually large magnitude(Col. 9, lines 15 –25, the examiner notes that a symbol is a byte, and a byte is made up of 8 bits, in order to alter or manipulate a byte, the bits or the higher order bits of the byte are manipulated, which is and the only way to alter a data byte into a error symbol, which will then replace a correctable data byte in the codeword according to the present invention, furthermore in plain meaning altering a data byte, also means altering its higher order bits.),

and the remaining:

- lower order bits of each data byte of the plurality of data bytes are altered such that, on decoding, the altered codeword will generate an uncorrectable error identifying syndrome(Col. 9, lines 15 –25, the examiner notes that a symbol is a byte, and a byte is made up of 8 bits, in order to alter or manipulate a byte, the bits or the lower order bits of the byte are manipulated, which is and the only way to alter a data byte into a error symbol, which will then replace a correctable data byte in the codeword according to the present invention, in plain meaning altering a data byte, also means altering its lower order bits.),

and wherein:

- a corrupting vector is formed which has the same format as the selected codeword, the corrupting vector having altered values imposed on a codeword in which all of the data values are zero(Col. 9, lines 15 – 25, the examiner notes that the corrupting vector, or codeword is a collection of bytes or collection of bits; error symbols are a collection of

invalid bytes or bits, thus a corrupting vector can be considered as a invalid error byte or symbol or bit pattern, that are placed into the codeword intentionally to render the codeword uncorrectable by a error correction unit, thus preventing an illegal copy from being copied efficiently. The examiner further notes that a codeword that has all data values of zero, the error correction unit would consider the codeword to be without errors if decoded by the error correction unit that would be present in a CD – ROM, or digital recording device, furthermore, the reference teaches a codeword that would normally be correctable(i.e. no errors or are present , until a error symbol or error or invalid byte is inserted to the codeword to make it uncorrectable to the error correction unit, therefore it can be assumed that the codeword as zero data byte values, before it is altered to be come uncorrectable.),

and further comprising:

- XORing the corrupting vector with the selected codeword whereby values in the selected codeword are XORed with the values in the corrupting vector to form the uncorrectable altered codeword (Col. 9, lines 15 – 25, the examiner notes that the operation of exclusive –or or Xoring is the same as Xoring a codeword with all data byte values being zero and a corrupting vector that could take on any value and always have the end result being a uncorrectable codeword when decoded by a error correcting unit. Exclusive – or , can take the operation of the following: 1 Xor 1 = 0 or 1 xor 0 = 1, the analogy being expressed is that if a codeword were equal to zero or the values of the data bytes were always being zero and the corrupting vector being a one or some other data value that will always be considered a error symbol or error byte, when the codeword and the

corrupting vector are Xored together and the end result will always be a codeword that is uncorrectable, this is fact constitutes an Xor operation.)

Claim(s) 8. A method of copy protecting encoded digital data, wherein:

- the encoded digital data has been subjected to error correcting encoding and is arranged in codewords, each codeword containing data bytes and parity values(Col. 9, lines 15 – 25, the examiner notes that ECC (error correction codeword), meaning that error correction encoding is to take place; to one of ordinary skill in the art, the ECC contains both symbols (data bytes) and parity bits; how the data bytes are being altered are that at specific CD medium locations, the correctable data bytes are being removed and being replaced with non-correctable data bytes. Thus, when an audio CD is read the error correction unit will mark those "altered" code words as uncorrectable, furthermore bypassing a error correction unit of a CD ROM, can be a means to prevent the unauthorized copying of the CD data.),

the method comprising:

- altering the values of the data in a plurality of data bytes in a selected codeword, to form an altered codeword, the nature of the altered values and the number of data bytes altered being chosen to render the altered codeword uncorrectable(Col. 9, lines 15 – 25, the examiner notes that ECC (error correction codeword), meaning that error correction encoding is to take place; to one of ordinary skill in the art, the ECC contains both

symbols (data bytes) and parity bits; how the data bytes are being altered are that at specific CD medium locations, the correctable data bytes are being removed and being replaced with non-correctable data bytes. Thus, when an audio CD is read the error correction unit will mark those "altered" code words as uncorrectable, furthermore bypassing a error correction unit of a CD ROM, can be a means to prevent the unauthorized copying of the CD data.),

and wherein:

- a corrupting vector is formed which has the same format as the selected codeword, the corrupting vector having altered values imposed on a codeword in which all of the data values are zero(Col. 9, lines 15 – 25, the examiner notes that the corrupting vector, or codeword is a collection of bytes or collection of bits; error symbols are a collection of invalid bytes or bits, thus a corrupting vector can be considered as a invalid error byte or symbol or bit pattern, that are placed into the codeword intentionally to render the codeword uncorrectable by a error correction unit, thus preventing an illegal copy from being copied efficiently. The examiner further notes that a codeword that has all data values of zero, the error correction unit would consider the codeword to be without errors if decoded by the error correction unit that would be present in a CD – ROM, or digital recording device, furthermore, the reference teaches a codeword that would normally be correctable(i.e. no errors or are present , until a error symbol or error or invalid byte is inserted to the codeword to make it uncorrectable to the error correction unit, therefore it can be assumed that the codeword as zero data byte values, before it is altered to be come uncorrectable.)

and further comprising:

- XORing the corrupting vector with the selected codeword whereby values in the selected codeword are XORed with the values in the corrupting vector to form the uncorrectable altered codeword (Col. 9, lines 15 – 25, the examiner notes that the operation of exclusive –or or Xoring is the same as Xoring a codeword with all data byte values being zero and a corrupting vector that could take on any value and always have the end result being a uncorrectable codeword when decoded by a error correcting unit. Exclusive – or , can take the operation of the following: 1 Xor 1 = 0 or 1 xor 0 = 1, the analogy being expressed is that if a codeword were equal to zero or the values of the data bytes were always being zero and the corrupting vector being a one or some other data value that will always be considered a error symbol or error byte, when the codeword and the corrupting vector are Xored together and the end result will always be a codeword that is uncorrectable, this is fact constitutes an Xor operation.)

The examiner notes that claim 8 is rejected under the same logic and reasoning that claim 23 is rejected under, furthermore the medium is merely the implementation of the method, which when both the method and the medium is executed the results will be exactly the same.

Claim(s) 10. A method as claimed in Claim 8 or Claim 9, wherein:

- a look up table containing a number of said corrupting vectors is provided, each of the corrupting vectors in the look up table being known to produce an uncorrectable error identifying syndrome(Col. 9, lines 50 – 57, the examiner notes that a table is made up of bit sequences, that does not represent any byte value or other assigned value.

The examiner notes that claim 24 is rejected under the same logic and reasoning that claim 10s rejected under, furthermore the medium is merely the implementation of the method, which when both the method and the medium is executed the results will be exactly the same.

Claim(s) 11. A method of copy protecting encoded digital data, wherein:

- the encoded digital data has been subjected to error correcting encoding and is arranged in codewords, each codeword containing data bytes and parity values(Col. 9, lines 15 – 25, the examiner notes that ECC (error correction codeword), meaning that error correction encoding is to take place; to one of ordinary skill in the art, the ECC contains both symbols (data bytes) and parity bits; how the data bytes are being altered are that at specific CD medium locations, the correctable data bytes are being removed and being replaced with non-correctable data bytes. Thus, when an audio CD is read the error correction unit will mark those "altered" code words as uncorrectable, furthermore bypassing a error correction unit of a CD ROM, which can be a means to prevent the unauthorized copying of the CD data.),

the method comprising:

- altering the values of the data in a plurality of data bytes in a selected codeword, to form an altered codeword, the nature of the altered values and the number of data bytes altered being chosen to render the altered codeword uncorrectable(Col. 9, lines 15 – 25, the examiner notes that ECC (error correction codeword), meaning that error correction encoding is to take place; to one of ordinary skill in the art, the ECC contains both symbols (data bytes) and parity bits; how the data bytes are being altered are that at specific CD medium locations, the correctable data bytes are being removed and being replaced with non-correctable data bytes. Thus, when an audio CD is read the error correction unit will mark those "altered" code words as uncorrectable, furthermore bypassing a error correction unit of a CD ROM, which can be a means to prevent the unauthorized copying of the CD data.),

the method:

- being for copy protecting digital data encoded for application to a CD(Col. 9, lines 38 – 45.),

wherein:

- four or more data bytes in selected C2 codewords are altered (Col. 11, lines 13 –28, the examiner notes that a total of 20 data symbol must be replaced in the C2 code word for efficient error correction override, which will make the CD not readable will copied illegally.)

The examiner notes that Claim 25, is also rejected under the same logic and reasoning as Claim 11, due to the fact that the medium is merely the implementation of the method, and when the medium is executed, the medium will produce the exact same result as the method if it was executed.

Claim(s) 12. A method as claimed in Claim 11, wherein:

- parity bytes of each C1 codeword incorporating a said altered data byte are additionally altered to render the said C1 codewords uncorrectable(Col. 11, lines 62 –67 & Col. 12, lines 1-8).

The examiner notes that Claim 26, is also rejected under the same logic and reasoning as Claim 12, due to the fact that the medium is merely the implementation of the method, and when the medium is executed, the medium will produce the exact same result as the method if it was executed.

Claim(s) 14. A data file containing:

- information for enabling encoded digital data to be copy protected, the encoded digital data being arranged in codewords containing data bytes and parity values, the information contained in the data file enabling the values of a plurality of data bytes in each of a number of selected codewords to be altered, where the nature of the altered values and the number of data bytes in each altered codeword are chosen to render the altered codeword uncorrectable (Col. 12, lines 32 – 41, the examiner notes that the

encoder takes in the data and changes it to the error or invalid data and does the interleaving of the error or invalid data.)

Claim(s) 15. A data file as claimed in Claim 14, which

- is arranged to be executable (col. 12, lines 32 – 41, the examiner notes that the laser writing control will implement the error symbols and interpolating onto a digital optical media, which by its nature is machine readable (i.e. CD player or CD ROM.)

Claim(s) 16. A medium on which copy protected encoded digital data has been stored, wherein:

- the medium carries the encoded digital data arranged in codewords containing data bytes and parity values(Col. 12, lines 32 – 41, the examiner notes that the system carries out the method of overriding error correction unit),

wherein:

- each of a plurality of data bytes in each of a number of selected codewords have had their values altered, the nature of the altered values and the number of data bytes altered in each altered codeword having been chosen to render the altered codeword uncorrectable (Col. 12, lines 32 – 41, the examiner notes that the system carries out the method of overriding error correction unit.)

6. Claim(s) 6, 7, 21, 22 are rejected under 35 U.S.C. 102(b) as being taught by Clark Jr. (US Patent # 3568148).

Clark Jr. teaches:

Claim(s) 6. A method of copy protecting encoded digital data, wherein:

- the encoded digital data has been subjected to error correcting encoding and is arranged in codewords, each codeword containing data bytes and parity values, the method comprising altering the values of the data in a plurality of data bytes in a selected codeword, to form an altered codeword, the nature of the altered values and the number of data bytes altered being chosen to render the altered codeword uncorrectable(Col. 7, lines 35 –39, the examiner notes that it inherent that if a vector or word or codeword is identified by the error correction unit or syndrome calculator as a "uncorrectable error," then the data bytes that make up the codeword have been altered in such a manner that the syndrome calculator flags this codeword as uncorrectable.),

and wherein:

- the nature of the altered values and the number of data bytes altered are chosen such that, on decoding, the altered codeword will generate an uncorrectable error identifying syndrome (Col. 7, lines 35 –39, the examiner notes that it inherent that if a vector or word or codeword is identified by the error correction unit or syndrome calculator as a "uncorrectable error," then the data bytes that make up the codeword have been altered in such a manner that the syndrome calculator flags this codeword as uncorrectable, furthermore the definition of a syndrome calculator according to the specification of the reference is that it decodes the codeword streams looking for error patterns.)

The examiner notes that claim 21 is rejected under the same logic and reasoning that claim 6 is rejected under, furthermore the medium is merely the implementation of the method, which when both the method and the medium is executed the results will be exactly the same.

Claim(s) 7. A method as claimed in Claim 6, wherein:

- the syndrome is one which, in the decoding process, causes an error locator polynomial to have no roots(Col. 3, lines 15 –53, the examiner notes that the logic circuit is the implementation of the polynomial in (Paragraphs: 15, 16), that is associated with the syndrome calculator, which decodes in input word and looks for all possible error patterns.)

The examiner notes that claim 22 is rejected under the same logic and reasoning that claim 7 is rejected under, furthermore the medium is merely the implementation of the method, which when both the method and the medium is executed the results will be exactly the same.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 13, 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sollish et al. (Patent # 6311305 B1) in view of Snelgrove et al. (US Patent # 6985 722 B1)

Sollish discloses inserting intentional errors or symbols in the codewords, rendering them uncorrectable to a error detection decoder, Col. 9, lines 15 – 25).

Sollish does not appear to explicitly disclose that the altered data bytes will provide audible clicks, when played back on a generic (i.e. any digital data recoder or digital recording system), there rendering the illegal copy of the digital content unaudible or unplayable.

However, Snelgrove discloses audible clicks when filtering out unwanted noise in a digital system, Col. 12, lines 39 –52.)

Sollish and Snelgrove are analyogous are because they are from the same field of endeavor by the fact that both deal with encoding/decoding or encrypting/decrypting a digital signal that is transmitted between two apparatuses, and if a signal is missing data bytes, there is a error correction encoding unit to correct the corrupted data bytes.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Sollish and Snelgrove before him or her, to modify the altering of the correctable data bytes with intentional error data bytes contained in codewords of Sollish to include the altering of the data bytes in such a manner that upon playback the altered data bytes would produce audible clicks of Snelgrove, because this would not convey to the person or persons the original data bytes in the manner as expected, instead the person or persons would

only hear a clicking noise, thus deterring the person or persons from making an illegal copy of digital data.

The suggestion of motivation for doing so would be altering the codewords in such a manner that altering the correctable data bytes and replacing them with invalid or error or uncorrectable data bytes thus rendering the codeword uncorrectable (i.e. preventing illegal copying of copyrighted material), also altering the codewords in such a manner that they produce a audible click on play back in a CD-ROM or Digital recording device, Col. 9, lines 1-9)

Therefore, it would have been obvious to combine Snelgrove and Sollish to obtain the invention as specified in the instant claims.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JOSEPH DEL SOLE
SUPERVISORY PATENT EXAMINER
6/8/07